WE CLAIM

1. A method of authenticating a pair of correspondents A,B to permit exchange of information therebetween, each of said correspondents having a respective private key a,b and a public key p_A,p_B derived from a generator α and respective ones of said private keys a,b, said method including the steps of

i) a first of said correspondents A selecting a first random integer x and exponentiating a function $f(\alpha)$ including said generator to a power $g^{(x)}$ to provide a first exponentiated function $f(\alpha)^{g(x)}$;

ii) said first correspondent A forwarding to a second correspondent B a message including said first exponentiated function $f(\alpha)^{g(x)}$;

iii) said correspondent B selecting a second random integer y and exponentiating a function $f'(\alpha)$ including said generator to a power $g^{(y)}$ to provide a second exponentiated function $f'(\alpha)^{g(y)}$;

iv) said second correspondent B constructing a session key K from information made public by said first correspondent A and information that is private to said second correspondent B, said session key K also being constructible by said first correspondent A for information made public by B and information that is private to said first correspondent A;

v) said second correspondent B generating a value h of a function F[ð,K] where F[ð,K] denotes a cryptographic function applied conjointly to ð and K and where ð is a subset of the public information provided by B thereby to bind the values of ð and K;

vi) said second of said correspondents B forwarding a message to said first correspondent A including said second exponential function $f'(\alpha)^{g(y)}$ and said value h of said cryptographic function F[ð,K];

vii) said first correspondent receiving said message and computing a session key K' from information made public by said second correspondent B and private to said first correspondent A;

viii) said first correspondent A computing a value h' of a cryptographic function

F[δ,K']; and

ix) comparing said values obtained from said cryptographic functions F to confirm their correspondence.

2. A method of claim 1 wherein said message forwarded by said first correspondent includes an identification of the first correspondent.

3. A method according to claim 1 wherein said message forwarded by said second correspondent includes an identification of said second correspondent.

4. A method according to claim 3 wherein said message forwarded by said first correspondent includes an identification of the first correspondent.

5. A method according to claim 1 wherein said first function $f(\alpha)$ including said generator is said generator itself.

6. A method according to claim 1 wherein said second function $f'(\alpha)$ including said generator is said generator itself.

7. A method according to claim 6 wherein said first function $f(\alpha)$ including said generator is said generator itself.

8. A method according to claim 1 wherein said first function including said generator $f(\alpha)$ includes said public key p_B of said second correspondent.

9. A method according to claim 1 wherein said second function including said generator $f\alpha$ includes said public key p_A of said first correspondent.

10. A method according to claim 1 wherein said cryptographic functions F are hashes of δ and K.

11. A method of transporting a key between a pair of correspondents A,B to permit exchange of information therebetween, each of said correspondents having a respective private key a,b and a public key p_A,p_B derived from a generator α and respective ones of said private keys a,b, said method including the steps of

i) a first of said correspondents A selecting a first random integer x and exponentiating a function f(α) including said generator to a power $g^{(x)}$ to provide a first exponentiated function $f(\alpha)^{g(x)}$;

ii) said first correspondent A forwarding to a second correspondent B a message including said first exponentiated function $f(\alpha)^{g(x)}$;

iii) said second correspondent B constructing a session key K from information made public by said first correspondent A and information that is private to said second correspondent B, said session key K also being constructible by said first correspondent A from information made public by B and information that is private to said first correspondent A;

iv) both of said first correspondent A and said second correspondents B computing a respective value h,h' of function F[ð,K] where F[ð,K] denotes a cryptographic function applied to ð and K and where ð is a subset of the public information provided by one of said correspondents;

v) at least one of said correspondents comparing said values h,h' obtained from said cryptographic function F to confirm their correspondence;

12. A method of claim 11 wherein said message forwarded by said first correspondent includes an identification of the first correspondent.

13. A method according to claim 11 wherein said message forwarded by said first correspondent includes said value obtained from said cryptographic function by said first correspondent.

14. A method according to claim 11 wherein said values obtained from

said cryptographic functions are obtained from a hash of said public information and said session key K.

15. A method according to claim 11 wherein said first correspondent selects a pair of random integers x and t and generates a session key K as $f(\alpha)^{g(t)}$, and generates a value r from said first exponentiated function $f(\alpha)^{g(x)}$ which includes a factor exponentiating said public key p_B of said second correspondent B with said random integer t to be of the form $p_B^{E(t)}\alpha^{g(x)}$.

16. A method according to claim 15 wherein said first correspondent A generates a value s from a combination of said random integer x and said private key a and forwards said value of r and said value of s to said second correspondent B to permit said second correspondent B to recover said session key K using the private key b of said second correspondent B.

17. A method according to claim 16 wherein said random integer x and said private key a are combined to produce s such that s=x-ra mod (p-1).

18. A method according to claim 17 wherein said cryptographic function F is a hash of said public information ð and said session key K.

19. A method according to claim 18 wherein said public information ð is the public key p_A of said first correspondent A.